Amendments to the Drawings:

The attached three (3) Replacement sheets of drawings, including Figures 9 to 11, have corrected "SINGED" to "SIGNED", as suggested. No new matter has been added and support is found in the present application, including the specification. Approval and entry are respectfully requested, and withdrawal of the objections is respectfully requested.

REMARKS

Claims 2, 5, 8 and 11 are canceled without prejudice, claims 21 to 26 are added, and therefore claims 1, 3, 4, 6, 7, 9, 10 and 12 to 26 are now pending and being considered.

It is respectfully submitted that all of the presently pending claims are allowable, and reconsideration is respectfully requested.

Applicants note with appreciation the acknowledgement of the claim for foreign priority and the indication that all certified copies of the priority documents have been received.

The amendments to the paragraph beginning at line 8 of page 27 and the paragraph beginning at line 12 of page 27 of the Specification correct grammatical and/or typological errors. No new matter has been added and support is found in the present application. Approval and entry are respectfully requested.

Applicants thank the Examiner for considering the previously filed Information Disclosure Statements, 1449 papers, and cited references. With respect to paragraphs four (4) and five (5) of the Office Action, English Abstracts for JP 8-251157 and JP 9-205422 are provided herewith. Note, that the previous IDS indicates that JP 8-251157 corresponds to U.S. Patent No. 5,625,692, which the IDS indicates was provided as a translation. and that for JP 9-205422, the prior IDS indicates that the description corresponds to the JP 8-251157 reference. It is therefore respectfully requested that these two references be considered and made of record, since they were disclosed in the prior IDS.

With respect to paragraph seven (7) of the Office Action, the drawings were objected to because the word "singed" of the label of element 15 should be written as "signed." Replacement sheets for revised Figs. 9 to 11 have made this correction. No new matter has been added, and support is found in the specification. Approval and entry are respectfully requested.

With respect to paragraph eight (8) of the Office Action, the drawings are objected to because the Examiner asserts that reference to Fig. 6 on page 27, line 8 of the specification should refer instead to Fig. 7. Applicants traverse this assertion. While the selection referred to in the referenced portion of the specification may be shown in Fig. 7, the "m subsets I(0) . . ." referred to in the referenced portion are shown in Fig. 6. The referenced portion of the specification therefore properly refers to Fig. 6. Withdrawal of the objection is therefore respectfully requested.

With respect to paragraph nine (9) of the Office Action, the drawings are objected to because the Examiner asserts that reference characters 2, 15, 16, 17, 18, 19, and step 64 are not mentioned in the specification. Elements 2 and 15 are discussed at page 33, line 11, and page 34, line 10, respectively. The specification has been amended to refer to 16 of Fig. 2, 17 of Fig. 3, 18 and 19 of Fig. 4 and 64 of Fig. 7. No new matter has been added and support is found in the present application. Approval and entry are respectfully requested.

With respect to paragraph ten (10) of the Office Action, the drawings were objected to because they do not show the element (1) referred to in the specification. The specification has been amended to change "1" to "2" at line 35 of page 16. No new matter has been added. Approval and entry are respectfully requested.

It is therefore respectfully requested that the objections to the drawings be withdrawn.

With respect to paragraph twelve (12) of the Office Action, the requirement to amend the specification to include the material of Boneh et al. as referred to in the specification is traversed. The generation of partial digital signatures in the absence of a trusted third party is disclosed at page 2, line 33, to page 3, line 15, as is the generation method of partial digital signatures, which is described in detail at page 19, line 32, to page 21, line 14. the Boneh reference is merely cited as an example for generating integers. Withdrawal of the objection to the specification is therefore respectfully requested.

With respect to paragraph thirteen (13), claims 7, 10, and 15 to 20 are objected to for assertedly not including transitional phrases. Each of the claims recites "wherein: . . .". such that the colon indicates that "wherein" applies to all of the following phrases. Withdrawal of the objections to claims 7, 10, and 15 to 20 is therefore respectfully requested.

With respect to paragraph fourteen (14), claim 5 was objected to as depending from itself. As explained herein, claim 5 has been canceled without prejudice. It is therefore respectfully requested that this objection be withdrawn as moot.

With respect to paragraph fifteen (15), claims 2, 5, 8, and 11 are rejected under 35 U.S.C. § 112, second paragraph as assertedly omitting essential steps. How a transformation number is used in a transformation process for generating integrated digital signature is described ate pages 22 and 23, and the claimed subject matter of the independent claims provides that a least common multiple of predetermined values is used as the transformation number. While the rejections may not be agreed with in view of the foregoing, to facilitate matters, claims 2, 5, 8 and 11 have been canceled without prejudice.

With respect to paragraph sixteen (16), claims 1, 3, 7, 9, 13, 15, 17, and 19 were rejected under 35 U.S.C. § 102(b) as anticipated by Malkin, Michael et al. "Building Intrusion Tolerant Applications," Darpa Information Survivability Conference and Exposition, 2000 (the "Michael et al." reference).

> As regards the anticipation rejections of the claims, to reject a claim under 35 U.S.C. § 102, the Office must demonstrate that each and every claim feature is identically described or contained in a single prior art reference. (See *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991)). Still further, not only must each of the claim features be identically described, an anticipatory reference must also enable a person having ordinary skill in the art to practice the claimed subject matter, as discussed herein. (See *Akzo, N.V. v. U.S.I.T.C.*, 1 U.S.P.Q.2d 1241, 1245 (Fed. Cir. 1986)).
>
> As further regards the anticipation rejections, to the extent that the Office Action may be relying on the inherency doctrine, it is respectfully submitted that to rely on inherency, the Examiner must provide a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics *necessarily* flows from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; and see *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Int'f. 1990)). Thus, the M.P.E.P. and the case law make clear that simply because a certain result or characteristic may occur in the prior art does not establish the inherency of that result or characteristic. Accordingly, it is respectfully submitted that any anticipation rejection premised on the inherency doctrine must fail absent the foregoing conditions.

With respect to paragraph seventeen (17), claims 4, 6, 10, 12, 14, 16, 18, and 20 were rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of the "Malkin" reference and U.S. Patent No. 5,610,982 (the "Micali" reference).

With respect to paragraph eighteen (18), claims 2 and 8 were rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of the "Malkin" reference and U.S. Patent No. 4,405,829 (the "Rivest et al." reference).

With respect to paragraph nineteen (19), claims 5 and 11 were rejected under 35 U.S.C. § 103(a) as unpatentable over the combination of the "Malkin", "Micali", and "Rivest et al." references.

> In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a prima facie case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish prima facie obviousness, three criteria must be satisfied. First, there must be some suggestion or motivation to modify or combine reference teachings. In re Fine, 837 F.2d 1071, 5 U.S.P.Q.2d 1596 (Fed.

> Cir. 1988). This teaching or suggestion to make the claimed combination must be found in the prior art and not based on the application disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). Second, there must be a reasonable expectation of success. In re Merck & Co., Inc., 800 F.2d 1091, 231 U.S.P.Q. 375 (Fed. Cir. 1986). Third, the prior art reference(s) must teach or suggest all of the claim features. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974).
> . . .

While the rejections may not be agreed with, in view of the foregoing, to facilitate matters, each of the independent claims has been revised to provide that a "least common multiple of predetermined values is used as a transformation number in said transformation process.

In particular, the rewritten independent claims are based on the original dependent claims and the disclosure at page 27, line 8, to page 28, line 26, and Figs.6-8. More particularly, the partial digital signature number set selecting step is based on the disclosure at page 27, lines 8-11 and Fig.6. The signature verification step is based on the disclosure at page 27, lines 15-18. The incorrect partial digital signature existence determination step is based on the processes of Fig.7, and the incorrect partial digital signature specifying step is based on the processes shown of Fig.8. The result output step is understood since the present invention is related to a service for generating a digital signature for a digital document in which correct integrated digital signature should be output when the correct integrated digital signature is generated, especially in view of the fact that Figs.9-11 suggest the result output step.

In contrast, the MALKIN reference essentially corresponds to the "first conventional method" in the specification. Accordingly, as discussed in the specification, MALKIN concerns a system in which partial signature keys are generated by each of partial digital signature generation systems without using a third party, and partial information on the partial signature key is exchanged each other, then, digital signature can be generated if a predetermined number (threshold) of the partial digital signature generation systems operate properly.

By adopting the incorrect partial digital signature existence determination step and the incorrect partial digital signature specifying step as provided for in the amended independent claims, the presently claimed subject matter produces remarkable effects as compared with

the MALKIN method, as is essentially discussed at page 29, line 1, to page 31, line 4, and at page 36, line 30 to page 38, line 37, in the specification with reference to Figs.13 and 14.

In particular, with respect to the amended independent claims, including claim 1, as presented, the feature of claim 2 is incorporated into each of the independent claims. As explained herein, the presently claimed subject matter of claim 1, as presented (as well as the other independent claims) is characterized in that a least common multiple (LCM) of predetermined values is used as the transformation number.

The Office Action asserts that the Rivest reference suggests using LCM as a transformation number. However, Rivest uses LCM for generating a key based on two prime numbers p and q, and therefore it does not suggest using LCM as a transformation number in a transformation process for generating integrated digital signature based on partial digital signatures as provided for in the context of claim 1 as presented.. According to the presently claimed subject matter, as described in page 24 in the specification, time complexity for generating the integrated digital signature can be decreased.

The Micali reference also does not in any way disclose or even suggest these features of the claimed subject matter of claim 1 as presented , and its corresponding dependent claims, or any of the other independent claims 4, 7, 10 and 13 to 20 as presented (which have been rewritten like claim 1 as presented), as well as their respective dependent claims 3, 6 and 9.

It is respectfully submitted that it would not be obvious to modify MALKIN by using the algorithm of Rivest since Rivest does not suggest using LCM as a transformation number in a transformation process for generating integrated digital signature, as provided for in the context of claim 1 as presented (and dependent claim 3), as well as claims 4 (and dependent claim 6), 7 (and dependent claim 9), 10 and 13 to 20

New claims 21 to 26 do no add any new matter and are supported by the present application, including the specification. With respect to the new claims 21 to 26, MALKIN does not identically describe (or even suggest) the feature of the partial digital signature number set selecting step, and the integrated digital signature generating step including the incorrect partial digital signature existence determination step and the incorrect partial digital signature specifying step. The other references also do not in any way disclose or even suggest these features of the claimed subject matter of new claims 21 to 26.

It is therefore respectfully submitted that claims 1, 3, 4, 6, 7, 9, 10, and 12 to 26 are allowable.

Conclusion

It is therefore respectfully submitted that all of claims 1, 3, 4, 6, 7, 9, 10 and 12 to 26 are allowable. It is therefore respectfully requested that the objections and rejections be withdrawn, since all issues raised have been addressed and obviated. An early and favorable action on the merits is therefore respectfully requested.

Respectfully submitted,

Dated: 1/18/2006 By: _____

Aaron C. Deditch
Reg. No. 33,865

KENYON & KENYON LLP
One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646